

# **End-User Requirements for NetSign Middleware CAC Cryptographic Logon**

**August 2005**



**Submitted by**

**ARMY Information Assurance CAC/PKI Training**

**2110 Washington Boulevard, Suite 200**

**Arlington VA 22204**



## Contact Us

To contact IA CAC/PKI Training, please call 703-769-4500 (extension x4482). We welcome your input as to how this manual can be improved.

For other CAC/PKI Questions you may contact the CAC/PKI Help Desk

Web: <https://iacacpki.army.mil>

Phone: 703-769-4499

DSN: 327-4004

Toll Free: 1-866-738-3222

Fax: 703-769-7605

## Additional Help

You can find additional help:

- For CAC Card Issues, contact your local ID Issuance / MPD Organization
- For Card reader / middleware issues, contact your local DOIM
- For Email issues, check your account on AKO and/or contact your DOIM.

## Introduction

The purpose of this guide is to assist Common Access Card (CAC) user's verify they have all required components necessary to facilitate the use of CAC Cryptographic Logon (CCL).

## Background

A significant deterrent in the past for using the CAC to logon to network resources has been the difficulty of attaining timely DoD PKI Certificate Validation (CV) information of the CAC holder. The DoD infrastructure-supported CV solution (download of the entire DoD certificate revocation list) does not provide an adequate solution. The Army is currently working on a viable CV solution that will provide the necessary support to warrant the implementation of a CCL capability in the near future. Another major deterrent is that CCL requires a Windows 2003 network infrastructure with Active Directory (AD). The Army plans to have this infrastructure in place at most installations by summer of 2005. In addition, user workstations require smart card readers and middleware which is already widely implemented throughout the Army.

It is envisioned that a phased approach will be used to introduce the CCL capability. The initial phase was completed during a certificate validation (CV) operational assessment (OA) conducted at Fort Dix, New Jersey in January-February 2005. The CCL capability was successfully implemented during the OA and is still in use. The second phase will consist of conducting an early adopter fielding during the fall of 2005. The last phase, if approved, will allow deployment of the CCL capability Army-wide.

In order to avoid delays with future CCL implementations, we requested the Director of Information Management (DOIM), in conjunction with the Garrison Military Personnel Directorate (MPD)/ CAC issuance center; assist their local CAC user population to conform to the following user level requirements:

- (1) CAC's must be configured with three Public Key Infrastructure (PKI) certificates (identity, email signature and email encryption)
- (2) User's must know there 6-8 digit CAC PIN
- (3) User workstations must have functioning smart card readers and middleware (ActivCard 3.0 or greater or NetSign 4.2 or greater)
- (4) User workstations must have Windows 2000 or XP operating systems.



End-users are responsible for verifying items 1 - 3 above.



Contact your local MPD regarding CAC issues and your local DOIM for smart card and middleware issues.

## Required Desktop Equipment

Below is a listing of the components that you will need to have in order to use CCL:

- Computer system (desktop/laptop)
- Smart card reader
- Common Access Card (CAC)

## Verifying PKI Certificates

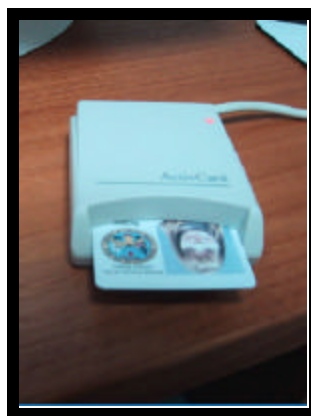


**Please contact your local CPR or MPD personnel for all CAC issues.**



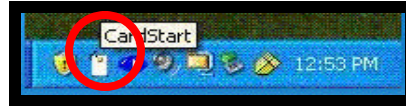
**Contact your local DOIM for all computer/ middleware issues.**

1. Locate your smart card reader and verify that it is connected to your computer; this can be accomplished by following the cord leading from the card reader to the computer. If you don't have a smart card reader, contact your local DOIM.



2. After logging on to your computer; locate the "System Tray ". It is located in the lower right quadrant of your computer display. This is the same area that the computers clock is displayed.

- Using your mouse, move your cursor over top of your middleware icon and double click using the left mouse button.



- At this point your middleware window should open, if it doesn't; repeat again.



Should repeated attempts fail, please contact your local DOIM for middleware problems.



If there are no icons displayed then please contact your local DOIM

- Insert your CAC in to the smart card reader. Your CAC should be inserted so that the picture is facing up and is visible.
- You may be asked to input your 6 – 8 digit CAC PIN.



### NetSign Pin Request



If you enter your CAC PIN incorrectly three times or you have forgotten your PIN please see your CAC PIN Reset (CPR) personnel or the local MPD in order to obtain a pin or have your PIN reset.

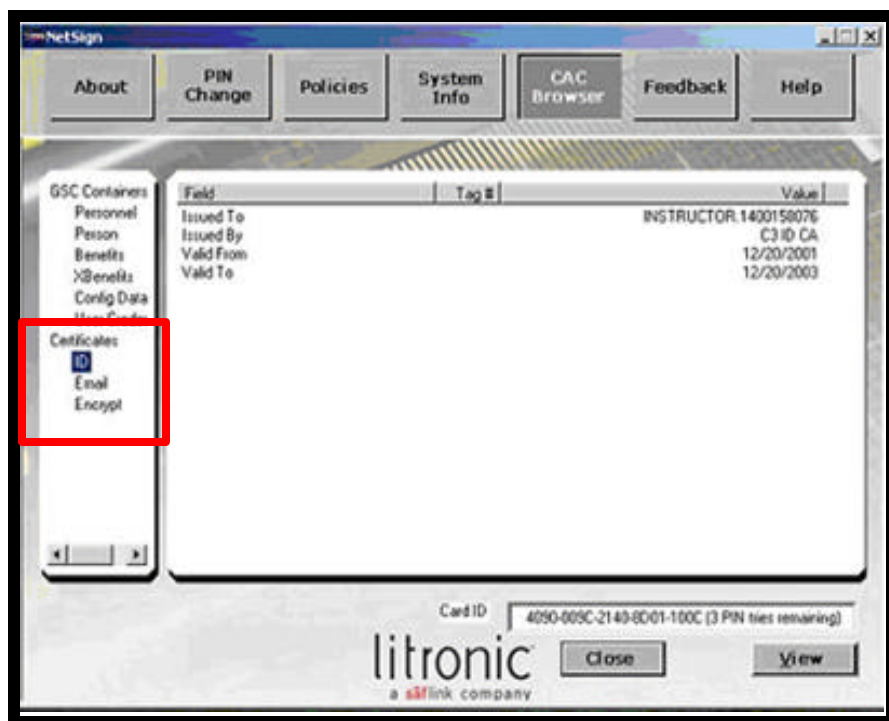


Please contact your local CPR or MPD personnel for CAC issues.

- Upon activating NetSign you'll Notice a pop-up window will appear.
- In the window you'll notice seven menu tabs located at the top of the window
- Using your mouse and the left mouse button select the "CAC Browser" menu.



10. Once the "CAC Browser" window opens you see two primary menus (GSC Containers and Certificates) with sub-menus listed below them.
11. Under the Certificates menu You should see the three required certificates.



12. If you have all three PKI certificates no further action is required.  
Please proceed to CAC Pin Check procedures.



If you do not see all three PKI certificates take the following steps.

## Missing Certificate?

### No PKI Certificates

1. If you already have an Army Knowledge Online (AKO) email address ([FName.LName@us.army.mil](mailto:FName.LName@us.army.mil)) go to your local MPD and have them add your PKI Identity certificate along with your two PKI email certificates ( email signature and email encryption), using your AKO email address, to your CAC.
2. If you don't have an AKO email address ([FName.LName@us.army.mil](mailto:FName.LName@us.army.mil)) go to the AKO website (<https://www.us.army.mil/suite/login/welcome.html>) and follow the instructions to obtain an AKO email address. Go to your local MPD and have them add your PKI Identity certificate along with your two PKI email certificates (email signature and email encryption), using your AKO email address, to your CAC.
3. Have the MPD verify that you now have all three PKI certificates.
4. This concludes the ActivCard portion please proceed to the CAC Pin Check procedure.

### Only have a PKI Identity certificate

1. If you already have an Army Knowledge Online (AKO) email address ([FName.LName@us.army.mil](mailto:FName.LName@us.army.mil)) go to your local MPD and have them add your two PKI email certificates ( email signature and email encryption), using your AKO email address, to your CAC.
2. If you don't have an AKO email address ([FName.LName@us.army.mil](mailto:FName.LName@us.army.mil)) go to the AKO website (<https://www.us.army.mil/suite/login/welcome.html>) and follow the instructions to obtain an AKO email address. Go to your local MPD and have them add your two PKI email certificates (email signature and email encryption), using your AKO email address, to your CAC.
3. Ensure to have the MPD verify that you now have all three PKI certificates.  
This concludes the NetSign portion please proceed to the CAC Pin Check procedure.

## CAC Pin Check

In the proceeding procedures you were ask to verify your certificates, during the process you may have had to enter your "Pin". In this case you will not receive a prompt to enter your pin again as long as you have not removed your CAC from the card reader.

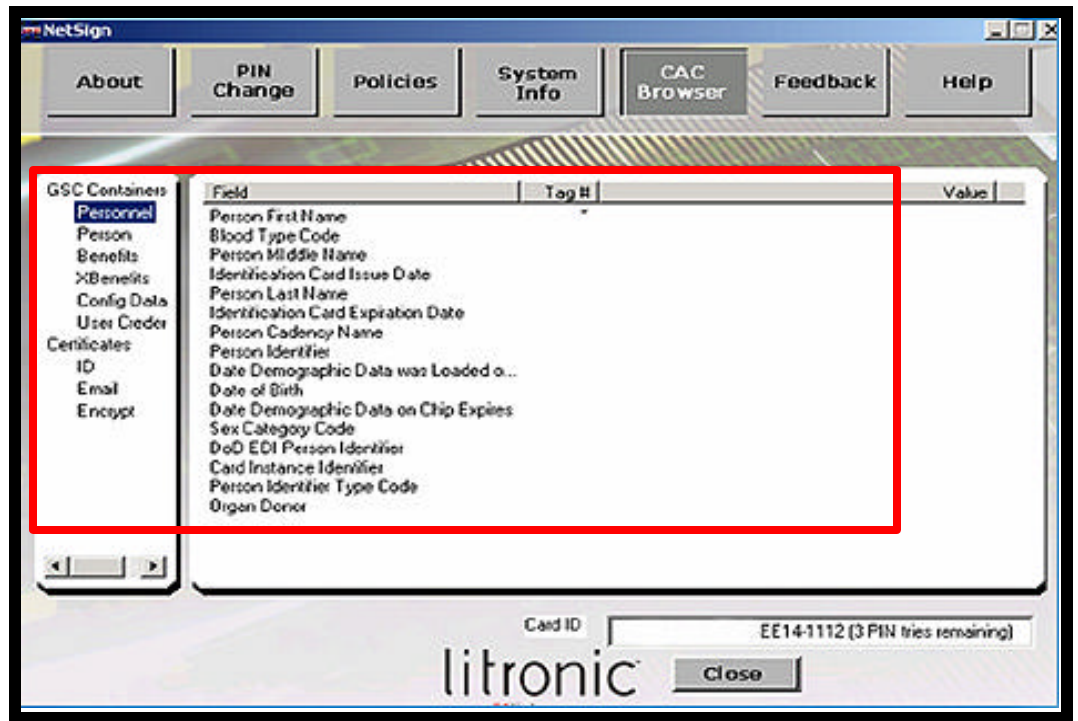
1. With your Middleware window open select the "Personnel" menu option by double clicking your left mouse button.



2. The "Pin Request" window will appear.



3. Enter your 6-8 digit pin.
4. Once you have properly entered the pin you will be able to view all your personnel data



5. This concludes the NetSign CAC Pin Check



\*\*\*This Page Intentionally Left Blank\*\*\*